A method and an electrical device for efficient multi-rate pseudo random noise (PN) sequence generation.

The present invention relates to an electrical device for generating a multi-rate PN sequence comprising:

- sequence generation means adapted to output a plurality of sequence values on the basis of a step control signal (S_t).

The present invention also relates to a method of generating a multi-rate PN sequence comprising the step of:

- generating a plurality of sequence values on the basis of a step control signal (S_t).

Pseudo random noise sequences (PN sequences) are used in many cryptographic and communications applications to provide randomly appearing symbols. Typically, cryptographic applications are methods to provide confidentiality of transmitted information through the use of stream ciphers. In communications systems PN sequences may e.g. be used as spreading sequences in spread-spectrum communications systems where they determine the hop sequence and/or the direct spreading sequence.

In general a receiver of a spread-spectrum communications system will receive a digital signal/bit stream transmitted over a single carrier frequency which is combined from a digital signal/bit stream containing information such as a digitized voice and from a PN sequence used to code or encrypt the transmission. Typically, the length of the PN sequence stream is much larger than the length of the information stream thereby,

complicating identification of ciphers containing the actual information.

In the prior art, the PN sequences are sometimes derived by using a maximal length polynomial. Constructions, whether hardware or software implemented, which form PN sequences, in this manner are sometimes referred to as m-sequence generators. It is well known that the randomness properties of the sequences generated by the m-sequence generators are very limited as a result of a linear relationship between the symbols of the sequence. This enables prediction of the next symbol given sufficiently many but small number of previous symbols. This is not desirable in various applications, and hence there is a need for efficient techniques to enhance the unpredictability.

Clock control of the m-sequence generator is a well-known method that can be used to increase the unpredictability of m-sequence generators. The most frequent method of clock control is that of introducing two modes of operation in an m-sequence generator. In one mode the generator outputs the previously produced symbol, and in the other mode the generator outputs the next symbol from the m-sequence. The current mode can advantageously be determined by another PN sequence. Output bits generated by a clock controlled m-sequence generator form the PN sequences which are used, inter alia, to encrypt or spread an information signal.

The abovementioned method of clock control, also sometimes referred to as the stop-and-go method, is especially used in hardware realisations where it is easy to implement this stop-and-go method. However, the randomness properties of the resulting sequence, although less predictable, are impaired by the fact that the

output sequence contains repetitions of previous symbols. This may obviated by using a step-once or step-twice ((1,2)-step) scheme, i.e. a basic m-sequence generator generates the next symbol (mode 1) or the symbol after the next symbol (mode 2), instead of the stop-and-go scheme. When implementing such a clock controlled generator, the basic m-sequence generator is required to produce symbols at twice the rate of the rate needed for output symbols. Known solutions for this depend on the use of a higher internal clock rate for the basic m-sequence generator or on the use of a very complex hardware realisation of clock controlled basic m-sequence generators.

EP 0905611 A2 discloses a pseudorandom number generating method and pseudorandom number generator where a selector selects a pseudorandom number X_j (a single bit) from either one of two function generator outputs on the basis of a previous pseudorandom number X_{j-1}. The two function generators output data composed of a plurality of bits corresponding to state data held in a register.

Another selector selects one of the data outputs of the function generators on the basis of the previous pseudorandom number X_{j-1} and stores this in the register as state data.

The abovementioned pseudorandom generator in EP 0905611 A2 does not disclose a clock controlled multi-rate generator and is subject to the abovementioned deterioration of unpredictability, since a clock rate twice as high as the needed output rate is needed because only one symbol is output at a time.

US 5,878,075 discloses a method of and an apparatus for generating a pseudorandom noise sequence (PN sequence),

where a bit sequence of pseudorandom numbers is augmented by a extra bit in order to comply with the Interim Standard IS-95 for implementation of CDMA (Code Division Multiple Access), where a sequence of 2^{15} bits is required.

An object of the invention is to provide an electrical device for efficient multi-rate PN sequence generation of simplified construction which is capable of generating one or more m-sequences at a multi-rate.

This object is achieved by an electrical device of the aforementioned type, said the device further comprising:

- selection means adapted to select one of said plurality of sequence values on the basis of a select value (M_t), and
- step control means adapted to provide the step control signal (S_t).

Hereby, a flexible, efficient and cryptographically more secure generation of sequences of pseudorandom ciphers is provided, which avoids the use of multiple system clocks and only requires little additional hardware and thereby little additional power consumption.

In accordance with one embodiment of the device according to the invention, the select value (M_t) is provided on the basis of a clock control value/signal (C_t) and a previously generated select value (M_{t-1}).

In accordance with another embodiment, the step control signal (S_t) is provided on the basis of a clock control value/signal (C_t) and a previously generated select value (M_{t-1}).

In a preferred embodiment, the plurality of sequence values is two, the step control signal (S_t) is calculated as $S_t = (C_t + M_{t-1})$ DIV 2 and the select value (M_t) is calculated as $M_t = (C_t + M_{t-1})$ MOD 2.

Hereby a (1,2)-step clock controlled m-sequence generator is provided with very little additional hardware.

Alternatively, the plurality of sequence values is four and the select value (M_t) is calculated as $M_t = (C_t + M_{t-1})$ MOD 4 and the step control signal (S_t) is calculated as $S_t = (C_t + S_t)$ DIV 4.

Hereby an efficient (1,2,3,4)-step clock controlled m-sequence generator is provided.

In general any N-step clock controlled m-sequence generator may be provided according to this invention, where $N \geq 2$. Accordingly the select value (M_t) may be calculated as $M_t = (C_t + M_{t-1})$ MOD N and the step control signal (S_t) may be calculated as $S_t = (C_t + S_t)$ DIV N.

Hereby an efficient N-step clock controlled m-sequence generation method is provided which an unpredictability that grows with N.

In an embodiment the sequence generation means is a windmill polynomial sequence generator.

In yet another embodiment the sequence generation means comprises:

- a plurality of delay elements,
- step control means receiving a next block control signal as input, and
- sum elements,

where each delay element is connected to another and two of them are additionally connected to themselves via a sum element.

Hereby, a very simple and efficient implementation of a windmill polynomial sequence generator is provided.

Another object of the invention is to provide a method of efficient multi-rate PN sequence generation of simplified complexity which is capable of generating one or more m-sequences at a multi-rate.

This object is achieved by a method of the aforementioned type, said method further comprising the steps of:

- providing a select value (M_t),
- providing the step control signal (S_t), and

selecting one of said plurality of sequence values on the basis of the select value (M_t).

In this way a method is provided which efficiently provides a PN sequence with enhanced unpredictability but with a small additional computational effort.

In accordance with one embodiment of the method according to the invention, the select value (M_t) is provided on the basis of a clock control value/signal (C_t) and a previously generated select value (M_{t-1}).

In accordance with another embodiment, the step control signal (S_t) is provided on the basis of a clock control value/signal (C_t) and a previously generated select value (M_{t-1}).

In a preferred embodiment, the plurality of sequence values is two, the step control signal (S_t) is calculated

as $S_t = (C_t + M_{t-1})$ DIV 2 and the select value (M_t) is calculated as $M_t = (C_t + M_{t-1})$ MOD 2.

Hereby a (1,2)-step clock controlled m-sequence generation method is provided with very little additional computational effort.

Alternatively, the plurality of sequence values is four and the select value (M_t) is calculated as $M_t = (C_t + M_{t-1})$ MOD 4 and the step control signal (S_t) is calculated as $S_t = (C_t + S_t)$ DIV 4.

Hereby an efficient (1,2,3,4)-step clock controlled m-sequence generation method is provided which is even more unpredictable.

In general any N-step clock controlled m-sequence generator may be provided according to this invention, where $N \geq 2$. Accordingly the select value (M_t) may be calculated as $M_t = (C_t + M_{t-1})$ MOD N and the step control signal (S_t) may be calculated as $S_t = (C_t + S_t)$ DIV N.

Hereby an efficient N-step clock controlled m-sequence generation method is provided which an unpredictability that grows with N.

In one embodiment the plurality of sequence values is generated by a windmill polynomial sequence generator.

The present invention also relates to the use of the method and/or electrical device mentioned above in a portable device. In a preferred embodiment the portable device is a mobile telephone.

Hereby, efficient and more safe encryption of digitized speech may be obtained.

Additionally, the reduced complexity of the hardware needed saves power which is especially important in e.g. a mobile telephone.

The present invention will now be described more fully with reference to the drawings, in which

Figure 1 illustrates a functional block diagram of a prior art (1,2)-step clock controlled m-sequence generator;

Figure 2 illustrates a functional block diagram of a windmill generator;

Figure 3 schematically illustrates a combination of a windmill generator and a Clock and Select system (CS system);

Figure 4 shows one realisation of the CS system shown in Figure 3;

Figure 5 shows a preferred realisation of ADD, MOD 2, and DIV 2 operations in hardware;

Figure 6 shows a generalisation of the bi-rate method described to a quaternary-rate (1,2,3,4)-step clock controlled m-sequence generator;

Figure 7 shows a generalized embodiment of a clock controlled m-sequence generator;

Figure 8 shows a flow chart of the method according to the invention;

Figure 9 shows the preferred embodiment of the invention, which may contain the electrical device and/or use the method according to the present invention;

Figures 10a and 10b show two exemplary implementations of a system using the method and/or device according to the invention.

Figure 1 illustrates a functional block diagram of a prior art (1,2)-step clock controlled m-sequence generator (101). This exemplary generator (101) outputs PN sequence symbols Z_t (102). The generator (101) has L=5 delay elements (103) each connected to step control means (104) receiving a clock control signal C_t (105) where t denotes the time instants 0, 1, 2,…. In this way each element (103) is clock controlled by a sequence $C = C_0, C_1, C_2, C_3,\ldots$, where each symbol represents the value 1 or 2, i.e. $C_t \in \{1,2\}$.

As will be seen, every value in the delay element (103) is shifted to the right at each time instant, except the value of the (from left to right) first element (103) which updates to the sum (without a carry) of the values of the second and the fifth delay elements (103) by an adding element (106).

If the m-sequence generator (101) steps once every time instant, the generator (101) will produce the simple sequence $X = X_0, X_1, X_2, X_3,\ldots$. With the shown initial values of the delay elements (103) (from left to right 0, 0, 1, 1, 0) the output sequence will be X = 1, 1, 0, 0, 0, 1, 1, 1,…. But if the stepping is controlled by the values of the symbols of C the following output sequence $Z = Z_0, Z_1, Z_2, Z_3,\ldots$, will be produced:

$$Z_t = X_{\sigma(t)} \qquad t = 0, 1, 2, 3,\ldots,$$

where

$$\sigma(t) = \Sigma_i C_i \qquad C_t \in \{1,2\},$$

and the sum Σ goes from i=0 to i=t-1. In other words, the next symbol Z_j is equal to either the next symbol X_k (if $C_t = 1$) or the next symbol again X_{k+1} (if $C_t = 2$). As an example, the sequence $Z_0 = X_0$, $Z_1 = X_2$, $Z_2 = X_4$, $Z_3 = X_6$, $Z_4 = X_7$ will be output if $C_0 = 2$, $C_1 = 2$, $C_2 = 2$, $C_3 = 1$.

In this way the unpredictability of the PN sequence Z_t (102) will be enhanced but creates the need for a clock rate for producing X_t which is twice as fast as the rate desired for Z_t, since two symbols of X must be calculated for each symbol of Z. The faster clock rate needed results in more circuitry and/or multiple system clocks.

Figure 2 illustrates a functional block diagram of a windmill generator (201). This is a windmill realisation of the m-sequence generator shown in Figure 1. Shown are L=5 delay elements (103) with step control means (104) connected to a next block control signal (202). The windmill generator (201) will output a sequence of the symbols $Z = Z_0, Z_1, Z_2, Z_3, \ldots$ in blocks of two tuples (Z_{2t}, Z_{2t+1}) (205, 206) for $t = 0, 1, 2, \ldots$. For each time instant a two tuple is generated if the next block control signal (202) is enabled, i.e. true/1. If the next block control signal (202) is disabled, i.e. false/0, the generator repeats the previous block, i.e. does not step to the next block.

The values of the delay elements (103) are shifted from the left to the right at each time instant, except the value of the (from left to right) first element which updates to the sum (without a carry) of the values of itself and the fifth delay elements (103) by an adding element (203), and except the third element which updates to the sum (without a carry) of the values of itself and

the previous/second element (103) by an adding element (204).

As an example, the initial values shown from left to right (0, 1, 0, 1, 0) will generate the following output sequence Z_{2t}(205) = 1, 0, 0, 1, 1, 0, 1 and Z_{2t+1}(206) = 1, 0, 1, 1, 1, 0, 1 for t = 0...6, if the next block control signal (202) is enabled.

In this way the need for extra circuitry and/or an extra system clock of higher rate is avoided, since a tuple of two values (Z_{2t}, Z_{2t+1}) of the PN sequence will be generated for each time instant, i.e. at each clock cycle.

Figure 3 schematically illustrates a combination of a windmill generator (201) and a Clock and Select system (301). The Clock and Select system (301), denoted CS system in the following, will be described in greater detail for one realisation in connection with Figure 4. The windmill generator (201) corresponds to the one shown in Figure 2.

The windmill generator (201) generates blocks/tuples of size v. In this exemplary embodiment the blocks are of the size v = 2, but blocks of other sizes are also within the scope of the present invention, as will be described later in connection with Figures 6 and 7.

This combination of the windmill generator (201) and the CS system (301) will generate a multi-rate clock controlled m-sequence.

The output symbols from the windmill generator (201), now denoted X_{2i} (302) and X_{2i+1} (303), are sent to the CS system (301). The windmill generator (201) receives a

step control signal S_t (304) which corresponds to the next block signal (202) in Figure 2.

The CS system (301) is responsible for the pacing of the windmill generator (201) by providing the step control signal S_t (304) and for selecting one of the two output symbols X_{2i} (302) and X_{2i+1} (303). The selected symbol is the final output symbol Z_t (305).

The CS system (301) receives a clock control signal C_t (306) which paces the CS system (301), since one set of symbol X_{2i} (302) and X_{2i+1} (303) and thereby one output symbol Z_t (305) will be generated for each value of the clock control signal C_t (306). One detailed embodiment of the CS system (301) will be explained in connection with Figure 4.

In this way, one cipher of the PN sequence will be generated for each clock cycle. The resulting PN sequence has a high degree of unpredictability since no linear relationship between the output ciphers exists, i.e. either the next symbol or the next symbol again is output. The output is obtained at the same rate as the input clock rate (C_t) without the need for multiple clocks and by very little additional hardware.

Figure 4 shows one realisation of the CS system (301) shown in Figure 3. This realisation of the CS system (301) in combination with the windmill generator (201) will result in a (1,2)-step clock controlled m-sequence generator.

Shown is selection means (401) adapted to select one of the two symbols X_{2i} (302) and X_{2i+1} provided by the windmill generator (201). The selection is done on the basis of a previously generated select value M_{t-1} (406)

(generated in the prior time instant as described later). If the previously generated select value M_{t-1} (406) is false/0 then one symbol from the windmill generator is selected, and if the value M_{t-1} (406) is true/1 the other symbol is selected. In the shown example, the symbol X_{2i} (302) is chosen for M_{t-1} (406) being false and X_{2i+1} is chosen for M_{t-1} (406) being true, but it could also be vice versa. The selected symbol is the final output symbol Z_t (305).

The previously generated select value M_{t-1} (406) is received from a delay element D (403) which keeps a newly generated select value M_t (407) for one time instant/clock cycle.

The clock control signal value C_t (306), pacing the CS system, is added by addition means (402) to the previously generated select value M_{t-1} (406). The sum (408) of C_t (306) and the previously generated select value M_{t-1} (406) can take the values 1,2,3.

From this sum (408) the new select value M_t (407) is derived by the MOD 2 means (404), i.e. M_t (407) = (C_t (306) + M_{t-1} (406)) MOD 2, and the new select value M_t (407) is kept in the delay element D (403), as described above.

The sum (408) is also used to derive the step control signal S_t (304) which is derived by the DIV 2 means (405), i.e. S_t (304) = (C_t (306) + M_{t-1} (406)) DIV 2. The step control signal S_t (304) is used by the windmill generator (201) to derive the two symbols X_{2i} (302) and X_{2i+1}, as described above.

In this way, the device shown in Figure 3 is implemented by little use of hardware.

Figure 5 shows a preferred realisation of ADD, MOD 2, and DIV 2 operations in hardware. The combination of ADD, MOD 2, and DIV 2 functionality may advantageously be realised in hardware by a 1 bit half-adder circuit (504).

The clock control signal C_t (305) is split into two signals, C_t^0 (503) and C_t^1 (502), by a logic circuit (501), preferably according to the following table:

C_t	C_t^0	C_t^1
0	1	0
1	0	1

In this way C_t^1 (502) is always equal to C_t (305) and C_t^0 (503) is always inverted to C_t (305).

C_t^0 (503) is added to the previously generated select value M_{t-1} (406) by the 1 bit half-adder circuit (504). The result consists of two signals (506, 407) which represents the carry and the sum of the addition, respectively. The sum corresponds to a MOD 2 function since it is performed without a carry. The sum is the select value M_t (407).

The carry signal (506) corresponds to a DIV 2 function and is used as input together with C_t^1 (502) (equal to C_t (305)) in an OR gate (505). The result of the OR gate (505) is the step control signal S_t (304) used to control the windmill generator (201).

This realisation greatly reduces the complexity of the hardware needed to provide a (1,2)-step clock controlled m-sequence generator.

Figure 6 shows a generalisation of the bi-rate method described to a quaternary-rate (1,2,3,4)-step clock controlled m-sequence generator. Shown are a windmill generator (601) and a CS system (602) which has been generalised from a bi-rate to a quaternary-rate.

The CS system (602) receives the clock control signal value C_t (603) now $\in$ {1, 2, 3, 4} and the windmill generator outputs four sequence values/symbols X_{4i} (604), X_{4i+1} (605), X_{4i+2} (606), X_{4i+3} (607) on the basis of the step control signal S_t (608).

Only one of the four sequence values (604 - 607) is selected as the final output symbol Z_t (609) of the PN sequence. The selection of one of the four symbols (604 - 607) in the CS system (602) is still provided on the basis of a previously generated select value M_{t-1}.

The step control signal S_t (608) is still provided on the basis of the clock control signal value C_t (603) and the previously generated select value M_{t-1} according to:

$$S_t = (C_t \ (603) + M_{t-1}) \ \text{DIV} \ 4,$$

and the new generated select value M_t is provided on the basis of the clock control signal value C_t (603) and the previously generated select value M_{t-1} according to:

$$M_t = (C_t \ (603) + M_{t-1}) \ \text{MOD} \ 4.$$

In this way a PN sequence with an even larger degree of unpredictability is provided with very little additional hardware.

Even PN sequences with a larger rate then four may be implemented, as described in connection with Figure 7,

using the same techniques and giving the same advantages as described above.

Figure 7 shows a generalized embodiment of a clock controlled m-sequence generator. Shown are a windmill generator (701) and a CS system (702) which has been generalised to a *N*-rate, where *N* is at least 2.

The CS system (702) receives the clock control signal value C_t (703) now $\in \{1, \ldots, N\}$ and the windmill generator outputs *N* sequence values/symbols X_{Ni} (704), X_{Ni+1} (705), ..., X_{Ni+N-1} (706) on the basis of the step control signal S_t (707).

Only one of the *N* sequence values (704 - 706) is selected as the final output symbol Z_t (709) of the PN sequence. The selection of one of the *N* symbols (704 - 706) in the CS system (602) is still provided on the basis of a previously generated select value M_{t-1}.

The step control signal S_t (707) may be provided on the basis of the clock control signal value C_t (703) and the previously generated select value M_{t-1} according to:

$$S_t = (C_t \ (703) + M_{t-1}) \ \text{DIV N},$$

and the new generated select value M_t may be provided on the basis of the clock control signal value C_t (703) and the previously generated select value M_{t-1} according to:

$$M_t = (C_t \ (703) + M_{t-1}) \ \text{MOD N}.$$

In this way, a PN sequence with an arbitrary large degree of unpredictability is provided with very little additional hardware.

The degree of unpredictability may be chosen according to a specific need for a given implementation.

Figure 8 shows a flow chart of the method according to the invention. The method generates a plurality of PN sequence values/symbols and selects one of these as output.

The method is initialised at step (801).

At step (802) a select value M_t is provided. The select value M_t may be calculated on the basis of a clock control value/signal C_t and a previously generated select value M_{t-1}. The clock signal C_t may e.g. be provided by an external control method or hardware circuit. The first time a select value is calculated, the previously generated select value may have the initial value of 0 or 1.

Preferably, the select value M_t is calculated as $M_t = (C_t + M_{t-1})$ MOD 2 for a plurality of sequence values being equal to two.

Alternatively, the select value M_t may be calculated as $M_t = (C_t + M_{t-1})$ MOD 4 for a plurality of sequence values being equal to four.

Other functions than MOD and DIV and other values than C_t and M_{t-1} may be provided.

At step (803) a control signal S_t is provided. The generated control value S_t is used to control the generation of sequence values at step (804).

The control signal S_t may be calculated on the basis of the clock control signal C_t and the previously generated select value M_{t-1}.

Preferably, the control value S_t is calculated as $S_t = (C_t + M_{t-1})$ DIV 2 for a plurality of sequence values being equal to two.

Alternatively, the control value S_t may be calculated as $S_t = (C_t + M_{t-1})$ DIV 4 for a plurality of sequence values being equal to four, but other functions and arguments may be provided.

The control value S_t and the select value M_t are calculated in this way on the basis of the same signals.

At step (804) a plurality of symbols/sequence values is generated. The generation of values may be done by any kind of sequence generator, e.g. a m-sequence generator, etc., but preferably the sequence generator is a windmill polynomial sequence generator. Alternatively, the generation may be done completely in software by methods corresponding to the mentioned generators.

The number of generated sequence values may vary according to how safe the method is to be, with a concomitant increase in the computational effort. Preferably, the number of generated values may be two or four, but any other number is just as applicable.

For two generated values, the next symbol and the next symbol again of the standard m-sequence generator are generated at the same time. For four values, the four next symbols will be generated, etc.

Preferably, the generation sequence values are controlled on the basis of the control signal S_t generated at step (802).

At step (805) one of the plurality of generated sequence values is selected and output as the next symbol in the output PN sequence. Preferably, the selection is done on the basis of the select value M_t. This selection of a value between a plurality of uncorrelated sequence values greatly enhances the unpredictability of the output sequence.

After execution of step (805) the method loops back to step (802). One loop is executed for each time step/instance.

In this way, a higher degree of unpredictability is obtained by very little computational effort.

Figure 9 shows a preferred embodiment of the invention, which may contain the electrical device and/or use the method according to the present invention. Shown is a mobile telephone (901) having display means (904), a keypad (905), an antenna (902), a microphone (906), and a speaker (903). By including the electrical device and/or the method according to the present invention a more safe and efficient encryption of speech signal is provided, just requiring very little additional hardware and/or additional computational effort.

Figures 10a and 10b show two exemplary implementations of a system using the method and/or device according to the invention.

Figure 10a shows a communications system (1001) comprising a first transmitting/receiving station (1003)

and a second sending/receiving station (1004) where information (1005) may be transmitted. The PN sequences generated by a (1,2)-step clock control m-sequence generator of an embodiment of the present invention may be used as a sub-component to encrypt information (1005) to be transmitted between the first transmitting/receiving station (1003) and the second transmitting/receiving station (1004).

Alternatively, a quaternary-rate (1,2,3,4)-step clock controlled m-sequence generator or other rate generators, as described in connection with Figures 6 and 7, may be provided in the system to improve the unpredictability even further.

In this way, safe transmission of information (1005) like data, digitized speech signals, etc. may be achieved by using less hardware, thereby reducing the costs and power consumption.

Figure 10b shows a transmitting/receiving station (1003) and a mobile terminal (901) which form a cellular communications system (1002). The information (1005) to be transmitted/received between the mobile terminal (901) and a network infrastructure (not shown) via the transmitting/receiving station (1003) may be encrypted through the use of a ciphering system that uses PN sequences generated by multi-rate clock controlled m-sequence generators.

Alternatively, a quaternary-rate (1,2,3,4)-step clock controlled m-sequence generator or other rate generators, as described in connection with Figures 6 and 7. may be provided in the system to improve the unpredictability even further.

In this way, safe transmission of information (1005) like data, digitized speech signals, etc. may be achieved by using less hardware, thereby reducing the costs and power consumption.

5